



**Quick Reference Guide V1.0 for the CMS
Required Security and Privacy Control
Baselines**
based on NIST SP 800-53 Rev.4

Access Control (AC)

ID	Control	Non-Cloud Baselines			FedRAMP / Cloud Baselines		
		L	M	H	L	M	H
AC-1	Access Control Policy and Procedures†	Y	Y	Y	Y	Y	Y
AC-2	Account Management	Y	Y- 1, 2, 3, 4, 5, 11, 12, 13	Y- 1, 2, 3, 4, 5, 7, 9, 10, 11, 12, 13	Y	Y- 1, 2, 3, 4, 5, 7, 9, 10, 11, 12, 13	Y- 1, 2, 3, 4, 5, 7, 9, 10, 11, 12, 13
AC-3	Access Enforcement	Y	Y	Y	Y	Y	Y
AC-4	Information Flow Enforcement	N	Y	Y	N	Y- 21	Y- 8, 21
AC-5	Separation of Duties	N	Y	Y	N	Y	Y
AC-6	Least Privilege	N	Y- 1, 2, 5, 9, 10	Y- 1, 2, 3, 5, 9, 10	N	Y- 1, 2, 5, 9, 10	Y- 1, 2, 3, 5, 7, 8, 9, 10
AC-7	Unsuccessful Logon Attempts	Y	Y	Y	Y	Y	Y- 2
AC-8	System Use Notification	Y	Y	Y	Y	Y	Y
AC-10	Concurrent Session Control	N	N	Y	N	Y	Y
AC-11	Session Lock	N	Y- 1	Y- 1	N	Y- 1	Y- 1
AC-12	Session Termination	N	Y	Y	N	Y	Y- 1
AC-14	Permitted Actions Without Identification or Authentication	Y	Y	Y	Y	Y	Y
AC-17	Remote Access	Y- 9	Y- 1, 2, 3, 4, 9	Y- 1, 2, 3, 4, 9	Y	Y- 1, 2, 3, 4, 9	Y- 1, 2, 3, 4, 9
AC-18	Wireless Access	Y	Y- 1	Y- 1, 4, 5	Y	Y- 1	Y- 1, 3, 4, 5
AC-19	Access Control for Mobile Devices	Y	Y- 5	Y- 5	Y	Y- 5	Y- 5
AC-20	Use of External Information Systemst†	Y	Y- 1, 2	Y- 1, 2	Y	Y- 1, 2	Y- 1, 2
AC-21	Information Sharing	N	Y	Y	N	Y	Y
AC-22	Publicly Accessible Content	Y	Y	Y	Y	Y	Y

Non-Mandatory: AC-9, AC-16,

Omitted: AC-13, AC-15, AC-23, AC-24, AC-25

Awareness and Training (AT)

ID	Control	Non-Cloud Baselines			FedRAMP / Cloud Baselines		
		L	M	H	L	M	H
AT-1	Security Awareness and Training Policy and Procedures†	Y	Y	Y	Y	Y	Y
AT-2	Security Awareness Training †	Y	Y- 2	Y- 2	Y	Y- 2	Y- 2
AT-3	Role-Based Security Training †	Y	Y	Y	Y	Y	Y- 3, 4
AT-4	Security Training Records †	Y	Y	Y	Y	Y	Y

Omitted: AT-5

Audit and Accountability (AU)

ID	Control	Non-Cloud Baselines			FedRAMP / Cloud Baselines		
		L	M	H	L	M	H
AU-1	Audit and Accountability Policy and Procedures†	Y	Y	Y	Y	Y	Y
AU-2	Audit Events	Y	Y- 3	Y- 3	Y	Y- 3	Y- 3
AU-3	Content of Audit Records	Y	Y- 1	Y- 1, 2	Y	Y- 1	Y- 1, 2
AU-4	Audit Storage Capacity	Y	Y	Y	Y	Y	Y
AU-5	Response to Audit Processing Failures	Y	Y	Y- 1, 2	Y	Y	Y- 1, 2
AU-6	Audit Review, Analysis, and Reporting	Y	Y- 1, 3	Y- 1, 3, 5, 6	Y	Y- 1, 3	Y- 1, 3, 4, 5, 6, 7, 10
AU-7	Audit Reduction and Report Generation	N	Y- 1	Y- 1	N	Y- 1	Y- 1
AU-8	Time Stamps	Y	Y- 1	Y- 1	Y	Y- 1	Y- 1
AU-9	Protection of Audit Information	Y	Y- 4	Y- 2, 3, 4	Y	Y- 2, 4	Y- 2, 3, 4
AU-10	Non-Reputation	N	N	Y	N	N	Y
AU-11	Audit Record Retention	Y	Y	Y	Y	Y	Y
AU-12	Audit Generation	Y	Y	Y- 1, 3	Y	Y	Y- 1, 3

Non-Mandatory: AU-16

Omitted: AU-13, AU-14, AU-15

Security Assessment and Authorization (CA)

ID	Control	Non-Cloud Baselines			FedRAMP / Cloud Baselines		
		L	M	H	L	M	H
CA-1	Security Assessment and Authorization Policies and Procedures†	Y	Y	Y	Y	Y	Y
CA-2	Security Assessments	Y	Y- 1	Y- 1, 2, 3	Y- 1	Y- 1, 2, 3	Y- 1, 2, 3
CA-3	System Interconnections	Y	Y- 5	Y- 5	Y	Y- 3, 5	Y- 3, 5
CA-5	Plan of Action and Milestones	Y	Y	Y	Y	Y	Y
CA-6	Security Authorization	Y	Y	Y	Y	Y	Y
CA-7	Continuous Monitoring	Y	Y- 1	Y- 1	Y	Y- 1	Y- 1, 3
CA-8	Penetration Testing	N	▲	Y	Y	Y- 1	Y- 1
CA-9	Internal System Connections	Y	Y	Y	Y	Y	Y

Omitted: CA-4

Configuration Management (CM)

ID	Control	Non-Cloud Baselines			FedRAMP / Cloud Baselines		
		L	M	H	L	M	H
CM-1	Configuration Management Policy and Procedures†	Y	Y	Y	Y	Y	Y
CM-2	Baseline Configuration	Y	Y- 1, 3, 7	Y- 1, 2, 3, 7	Y	Y- 1, 2, 3, 7	Y- 1, 2, 3, 7
CM-3	Configuration Change Control	N	Y- 2	Y- 1, 2	N	Y	Y- 1, 2, 4, 6
CM-4	Security Impact Analysis	Y	Y	Y- 1	Y	Y	Y- 1
CM-5	Access Restrictions for Change	N	Y	Y- 1, 2, 3	N	Y- 1, 3, 5	Y- 1, 2, 3, 5
CM-6	Configuration Settings	Y	Y	Y- 1, 2	Y	Y- 1	Y- 1, 2
CM-7	Least Functionality	Y	Y- 1, 2, 4	Y- 1, 2, 5	Y	Y- 1, 2, 5	Y- 1, 2, 5
CM-8	Information System Component Inventory	Y	Y- 1, 3, 5	Y- 1, 2, 3, 4, 5	Y	Y- 1, 3, 5	Y- 1, 2, 3, 4, 5
CM-9	Configuration Management Plan	N	Y	Y	N	Y	Y
CM-10	Software Usage Restrictions	Y	Y	Y	Y	Y- 1	Y- 1
CM-11	User-Installed Software	Y	Y	Y	Y	Y	Y- 1

Identity and Authentication (IA)

ID	Control	Non-Cloud Baselines			FedRAMP / Cloud Baselines		
		L	M	H	L	M	H
IA-1	Identification and Authentication Policy and Procedures†	Y	Y	Y	Y	Y	Y
IA-2	Identification and Authentication (Organizational Users)	Y- 1, 11, 12	Y- 1, 2, 3, 4, 8, 9, 11, 12	Y- 1, 2, 3, 4, 8, 9, 11, 12	Y- 1, 12	Y- 1, 2, 3, 4, 5, 8, 11, 12	Y- 1, 2, 3, 4, 5, 8, 11, 12
IA-3	Device Identification and Authentication	N	Y	Y	N	Y	Y
IA-4	Identifier Management	Y	Y	Y	Y	Y- 4	Y- 4
IA-5	Authenticator Management	Y- 1, 11	Y- 1, 2, 3, 11	Y- 1, 2, 3, 11	Y- 1, 11	Y- 1, 2, 3, 4, 6, 7, 8, 11, 13	Y- 1, 2, 3,

Physical and Environmental Protection (PE)

ID	Control	Non-Cloud Baselines			FedRAMP / Cloud Baselines		
		L	M	H	L	M	H
PE-1	Physical and Environmental Protection Policy and Procedures†	Y	Y	Y	Y	Y	Y
PE-2	Physical Access Authorizations	Y	Y	Y	Y	Y	Y
PE-3	Physical Access Control	Y	Y	Y- 1	Y	Y	Y- 1
PE-4	Access Control for Transmission Medium	N	Y	Y	N	Y	Y
PE-5	Access Control for Output Devices	N	Y	Y	N	Y	Y
PE-6	Monitoring Physical Access	Y	Y- 1	Y- 1,4	Y	Y- 1	Y- 1,4
PE-8	Visitor Access Records	Y	Y	Y- 1	Y	Y	Y- 1
PE-9	Power Equipment and Cabling	N	Y	Y	N	Y	Y
PE-10	Emergency Shutoff	N	Y	Y	N	Y	Y
PE-11	Emergency Power	N	Y	Y- 1	N	Y	Y- 1
PE-12	Emergency Lighting	Y	Y	Y	Y	Y	Y
PE-13	Fire Protection	Y	Y- 3	Y- 1,2,3	Y	Y- 2,3	Y- 1,2,3
PE-14	Temperature and Humidity Controls	Y	Y	Y	Y	Y- 2	Y- 2
PE-15	Water Damage Protection	Y	Y	Y- 1	Y	Y	Y- 1
PE-16	Delivery and Removal	Y	Y	Y	Y	Y	Y
PE-17	Alternate Work Site		Y	Y	N	Y	Y
PE-18	Location of Information System Components	N	N	Y	N	N	Y

Omitted: PE-7, PE-19, PE-20

Planning (PL)

ID	Control	Non-Cloud Baselines			FedRAMP / Cloud Baselines		
		L	M	H	L	M	H
PL-1	Security Planning Policy and Procedures†	Y	Y	Y	Y	Y	Y
PL-2	System Security Plan	Y	Y- 3	Y- 3	Y	Y- 3	Y- 3
PL-4	Rules of Behavior†	Y	Y- 1	Y- 1	Y	Y- 1	Y- 1
PL-8	Information Security Architecture	N	Y	Y	N	Y	Y

Omitted: PL-5, PL-6, PI-7, PL-9

Personnel Security (PS)

ID	Control	Non-Cloud Baselines			FedRAMP / Cloud Baselines		
		L	M	H	L	M	H
PS-1	Personnel Security Policy and Procedures†	Y	Y	Y	Y	Y	Y
PS-2	Position Risk Designation	Y	Y	Y	Y	Y	Y
PS-3	Personnel Screening	Y	Y	Y	Y	Y- 3	Y- 3
PS-4	Personnel Termination	Y	Y	Y- 2	Y	Y	Y- 2
PS-5	Personnel Transfer	Y	Y	Y	Y	Y	Y
PS-6	Access Agreements	Y	Y	Y	Y	Y	Y
PS-7	Third-Party Personnel Security	Y	Y	Y	Y	Y	Y
PS-8	Personnel Sanctions	Y	Y	Y	Y	Y	Y

Risk Assessment (RA)

ID	Control	Non-Cloud Baselines			FedRAMP / Cloud Baselines		
		L	M	H	L	M	H
RA-1	Risk Assessment Policy and Procedures†	Y	Y	Y	Y	Y	Y
RA-2	Security Categorization	Y	Y	Y	Y	Y	Y
RA-3	Risk Assessment	Y	Y	Y	Y	Y	Y
RA-5	Vulnerability Scanning	Y	Y- 1, 2, 5	Y- 1, 2, 4, 5	Y	Y- 1, 2, 3, 5, 6, 8	Y- 1, 2, 3, 4, 5, 6, 8, 10

Omitted: RA-4, RA-6

System and Services Acquisition (SA)

ID	Control	Non-Cloud Baselines			FedRAMP / Cloud Baselines		
		L	M	H	L	M	H
SA-1	System and Services Acquisition Policy and Procedures†	Y	Y	Y	Y	Y	Y
SA-2	Allocation of Resources	Y	Y	Y	Y	Y	Y
SA-3	System Development Life Cycle	Y	Y	Y	Y	Y	Y
SA-4	Acquisition Process	Y- 10	Y- 1, 2, 9, 10	Y- 1, 2, 9, 10	Y	Y- 1, 2, 8, 9, 10	Y- 1, 2, 8, 9, 10
SA-5	Information System Documentation	Y	Y	Y	Y	Y	Y
SA-8	Security Engineering Principles	N	Y	Y	N	Y	Y
SA-9	External Information System Services	Y	Y- 2	Y- 2	Y	Y- 1, 2, 4, 5	Y- 1, 2, 4, 5
SA-10	Developer Configuration Management	N	Y	Y	N	Y- 1	Y- 1
SA-11	Developer Security Testing and Evaluation	N	Y	Y	N	Y- 1, 2, 8	Y- 1, 2, 8
SA-12	Supply Chain Protection	N	N	Y	N	N	Y
SA-15	Development Process, Standards, and Tools	N	Y- 9	Y- 9	N	N	Y
SA-16	Developer-Provided Training	N	N	Y	N	N	Y
SA-17	Developer Security Architecture and Design	N	N	Y	N	N	Y

Non-Mandatory: SA-13, SA-21, SA-22

Omitted: SA-6, SA-7, SA-14, SA-18, SA-19, SA-20

System and Communications Protections (SC)

ID	Control	Non-Cloud Baselines			FedRAMP / Cloud Baselines		
		L	M	H	L	M	H
SC-1	System and Communications Protection Policy and Procedures†	Y	Y	Y	Y	Y	Y
SC-2	Application Partitioning	N	Y	Y	N	Y	Y
SC-3	Security Function Isolation	N	N	Y	N	N	Y
SC-4	Information in Shared Resources	N	Y	Y	Y	Y	Y
SC-5	Denial of Service Protection	Y	Y	Y	Y	Y	Y
SC-6	Resource Availability	N	N	N	N	Y	Y
SC-7	Boundary Protection	Y	Y- 3, 4, 5, 7	Y- 3, 4, 5, 7, 8, 18, 21	Y	Y- 3, 4, 5, 7, 8, 12, 13, 18	Y- 3, 4, 5, 7, 8, 10, 12, 13, 18, 20, 21
SC-8	Transmission Confidentiality and Integrity	N	Y- 1	Y- 1	N	Y- 1	Y- 1
SC-10	Network Disconnect	N	Y	Y	N	Y	Y

ID	Control	L	M	H	L	M	H
SC-12	Cryptographic Key Establishment and Management	Y	Y	Y- 1	Y	Y- 2, 3	Y- 1, 2, 3
SC-13	Cryptographic Protection	Y	Y	Y	Y	Y	Y
SC-15	Collaborative Computing Devices	Y- 1	Y- 1	Y- 1	Y	Y	Y
SC-17	Public Key Infrastructure Certificates	N	Y	Y	N	Y	Y
SC-18	Mobile Code	N	Y	Y	N	Y	Y
SC-19	Voice Over Internet Protocol	N	Y	Y	N	Y	Y
SC-20	Secure Name/Address Resolution Service (Authoritative Source)	Y	Y	Y	Y	Y	Y
SC-21	Secure Name/Address Resolution Service (Recursive or Caching Resolver)	Y	Y	Y	Y	Y	Y
SC-22	Architecture and Provisioning for Name/Address Resolution Service	Y	Y	Y	Y	Y	Y
SC-23</td							

Program Management (PM)

ID	Control	Non-Cloud Baselines			FedRAMP / Cloud Baselines		
		L	M	H	L	M	H
PM-1	Information Security Program Plant†	Y	Y	Y	Y	Y	Y
PM-2	Senior Information Security Officer†	Y	Y	Y	Y	Y	Y
PM-3	Information Security Resources	Y	Y	Y	Y	Y	Y
PM-4	Plan of Action and Milestones Process†	Y	Y	Y	Y	Y	Y
PM-5	Information System Inventory	Y	Y	Y	Y	Y	Y
PM-6	Information Security Measures of Performance†	Y	Y	Y	Y	Y	Y
PM-7	Enterprise Architecture†	Y	Y	Y	Y	Y	Y
PM-8	Critical Infrastructure Plan	Y	Y	Y	Y	Y	Y
PM-9	Risk Management Strategy	Y	Y	Y	Y	Y	Y
PM-10	Security Authorization Process	Y	Y	Y	Y	Y	Y
PM-11	Mission/Business Process Definition	Y	Y	Y	Y	Y	Y
PM-12	Insider Threat Program	Y	Y	Y	Y	Y	Y
PM-13	Information Security Workforce	Y	Y	Y	Y	Y	Y
PM-14	Testing, Training, and Monitoring	Y	Y	Y	Y	Y	Y
PM-15	Contacts with Security Groups and Associations	Y	Y	Y	Y	Y	Y
PM-16	Threat Awareness Program	Y	Y	Y	Y	Y	Y

Appendix J: Privacy Controls for Moderate and High Systems

Processing, Storing, or Transmitting PII and PHI

Authority and Purpose (AP)

AP-CMS-1	Authority and Purpose Policy and Procedures (Non-Mandatory) †
AP-1	Authority to Collect
AP-2	Purpose Specification

Accountability, Audit, and Risk Management (AR)

AR-CMS-1	Accountability, Audit, and Risk Management Policy and Procedures (Non-Mandatory) †
AR-1	Governance and Privacy Program †
AR-2	Privacy Impact and Risk Assessment †
AR-3	Privacy Requirements for Contractors and Service Providers †
AR-4	Privacy Monitoring and Auditing †
AR-5	Privacy Awareness and Training †
AR-6	Privacy Reporting
AR-7	Privacy-Enhanced System Design and Development
AR-8	Accounting of Disclosures

Data Quality and Integrity (DI)

DI-CMS-1	Data Quality and Integrity Policy and Procedures (Non-Mandatory) †
DI-1	Data Quality
DI-2	Data Integrity and Data Integrity Board

Data Minimization and Retention (DM)

DM-CMS-1	Data Minimization and Retention Policy and Procedures (Non-Mandatory) †
DM-1	Minimization of Personally Identifiable Information
DM-2	Data Retention and Disposal
DM-3	Minimization of PII Used in Testing, Training, and Research

Individual Participation and Redress (IP)

IP-CMS-1	Individual Participation and Redress Policy and Procedures (Non-Mandatory) †
IP-1	Consent
IP-2	Individual Access
IP-3	Redress
IP-4	Complaint Management

Security (SE)

SE-CMS-1	Security Policy and Procedures (Non-Mandatory) †
SE-1	Inventory of Personally Identifiable Information
SE-2	Privacy Incident Response

Transparency (TR)

TR-CMS-1	Transparency Policy and Procedures (Non-Mandatory) †
TR-1	Privacy Notice
TR-2	System of Records Notices and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information

Use Limitation (UL)

UL-CMS-1	Use Limitation Policy and Procedures (Non-Mandatory) †
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Legend

If an enhancement is listed (Y- x, where “x” is one or more numbers), the control is selected!

High	High Security Categorization	Y	Control selected
Mod	Moderate Security Categorization	Y- 1, 2, ...	Control enhancements selected
Low	Low Security Categorization	N	Control not selected

▲ Control/enhancement is required by CMS for any system designated as an HVA

† OCISO **inheritable hybrid** control/control enhancement. Each system must address system specific policies and procedures. Contact the OCISO ISSO for details.

Non-Mandatory Controls are controls that CMS recommends be considered but are not required under the minimal baseline. Business owners are encouraged to look at these controls for selection and implementation within their environment if risk dictates.

Omitted Controls are those controls that were deemed discretionary for implementation within CMS or have been withdrawn by NIST.

For cloud deployments, the minimal baseline is defined within the **FedRAMP Reference Guides**. These references are found at:

<https://www.fedramp.gov/resources/documents-2016/>

Tallies (Controls/Control Enhancements)

Standard Baselines	H: 195/178	M: 186/106	L: 139/12
Cloud Baselines	H: 194/249	M: 186/161	L: 139/9
Added to address PII/PHI	H: 20/10	M: 20/10	L: 20/10
Standard Baselines with Privacy	H: 215/188	M: 206/116	L: 159/22
Cloud Baselines with Privacy	H: 214/259	M: 206/171	L: 159/19